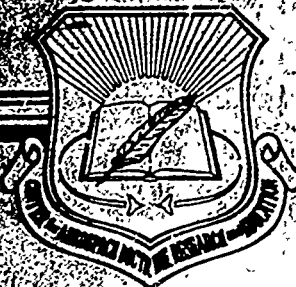


DTIC FILE COPY

(1)

AD-A224 640

DTIC
S ELECTE D
JUN 13 1980
B



Air Base Security

*Developing an
Operational Doctrine*

David C. Martin, Major, USAF

DISTRIBUTION STATEMENT A

Approved for public release;
Distribution Unlimited

90 06 12 054

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20563.

1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE		3. REPORT TYPE AND DATES COVERED	
4. TITLE AND SUBTITLE Air Base Security: Developing an Operational Doctrine				5. FUNDING NUMBERS	
6. AUTHOR(S) Major David C Martin, USAF					
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AUCADRE/PTP Maxwell AFB AL 36112-5532				8. PERFORMING ORGANIZATION REPORT NUMBER AU-ARI-89-4	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES					
12a. DISTRIBUTION / AVAILABILITY STATEMENT Public Release				12b. DISTRIBUTION CODE A	
13. ABSTRACT (Maximum 200 words) This study is a prolegomenon to an operational doctrine for air base security and a valuable guide to the people who will eventually prepare that document. <i>Keywords: Air Force Personnel; Military Doctrine.</i> (CP)					
14. SUBJECT TERMS				15. NUMBER OF PAGES 64 pages	
				16. PRICE CODE None	
17. SECURITY CLASSIFICATION OF REPORT UNCLAS	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLAS	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLAS	20. LIMITATION OF ABSTRACT NONE		

After you have read the research report, please give us your frank opinion on the contents. All comments—large or small, complimentary or caustic—will be gratefully appreciated. Mail them to: CADRE/RI, Building 1400, Maxwell AFB AL 36112-5532.



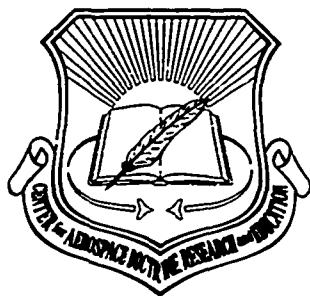
Air Base Security

Martin

Developing an Operational Doctrine

Cut along dotted line

Thank you for your assistance



Research Report No. AU-ARI-89-4

Air Base Security

Developing an Operational Doctrine

by

DAVID C. MARTIN, Major, USAF
Research Fellow
Airpower Research Institute

DTIC
ELECTE
JUN 13 1990
S B D

Air University Press
Maxwell Air Force Base, Alabama 36112-5532

April 1990

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

DISCLAIMER

This study represents the views of the author and does not necessarily reflect the official opinion of the Air University Center for Aerospace Doctrine, Research, and Education (AUCADRE) or the Department of the Air Force. This publication has been reviewed by security and policy review authorities and is cleared for public release.

This document is the property of the United States government and is not to be reproduced in whole or in part without permission of the commander, AUCADRE, Maxwell Air Force Base, Alabama.

Contents

Chapter	Page
DISCLAIMER	ii
FOREWORD	vii
ABOUT THE AUTHOR	ix
PREFACE	xi
1 WHY AIR BASE SECURITY OPERATIONAL DOCTRINE?	1
Calls for an Operational Doctrine	1
ABGD Doctrinal Requirements	1
Readiness Reporting Study	2
Innovation Initiatives	2
Regulatory Requirements	2
Defining Operational Doctrine	3
Holley's Methodology	3
An Air Base Security Operational Model	3
Levels of Threat	3
Spectrum of Conflict	4
Current Missions	4
Tying It Together	4
Notes	5
2 LEVELS OF THREAT	7
Lowering the Threshold: Basic Threats	7
Level I Threats	9
Level II Threats	9
Level III Threats	10
Notes	12
3 SPECTRUM OF CONFLICT	13
Spreading the Range: Primary Conflicts	14
Primary Criminal Conflicts	14
Primary Domestic Conflicts	14
Low-Intensity Conflicts	14
Insurgency/Counterinsurgency	15
Counterterrorism and Antiterrorism	15



Session For	
CS GRA&I	<input checked="" type="checkbox"/>
IC TAB	<input type="checkbox"/>
announced	<input type="checkbox"/>
ification	

Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

<i>Chapter</i>		<i>Page</i>
	Peacekeeping Operations	16
	Peacetime Contingency Operations	16
	Midintensity Conflicts: Conventional Warfare	16
	High-Intensity Conflicts: Nuclear Warfare	16
	Notes	17
4	CURRENT MISSIONS	19
	Law Enforcement	19
	Operations	19
	Administration and Reports	20
	Systems Security	21
	Command, Control, and Communications	21
	Priority Resource Security	21
	Air Base Ground Defense	22
	Command, Control, Communications, and Intelligence	22
	Internal Defense	22
	External Defense	23
	Information Security	23
	Information Security Program	23
	Personnel Security Program	23
	Industrial Security Program	23
	Classification Management	23
	Security Education Program	24
	Wartime Information Security Program	24
	Computer Security	24
	Communications Security	24
	Operations Security	24
	Notes	25
5	A RECOMMENDED PROCESS OF DOCTRINAL DEVELOPMENT	27
	Professor Holley and the Writing of Doctrine	27
	Phase 1: Collection	28
	Phase 2: Formulation	29
	Phase 3: Dissemination	29
	Applying Holley's Methodology to the Air Base Security Model	30
	Identifying Sources for Collection Phase	30
	Suggested Steps for the Formulation Phase	33
	The Official Dissemination Phase	34
	Conclusion	34
	Notes	34

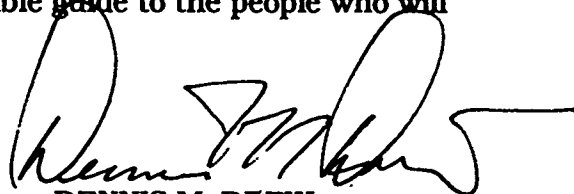
Appendix

Page

A	Definitions of Doctrine	39
B	Air Base Security Operational Doctrine (AFM 2-XZ): A Suggested Outline	45
	GLOSSARY	51

Foreword

Since their inception, the Air Force Security Police have been responsible for the security of US air bases worldwide. Toward that end, they have developed and conducted missions designed to safeguard Air Force assets during peace or war. Some readers may be surprised to learn that the Security Police have managed to do their job without benefit of an operational doctrine. Although that fact may suggest that they do not need a formal doctrine, there are certain advantages to writing down generalizations that are based on experience, especially for the purpose of instructing the rest of the Air Force in matters of security. Major Martin does not write such a doctrine, but he explains why we need one and gives us a methodology for writing it. In short, his study is a prolegomenon to an operational doctrine for air base security and a valuable guide to the people who will eventually prepare that document.



DENNIS M. DREW
Colonel, USAF
Director, Airpower Research
Institute

About the Author

Maj David C. Martin enlisted in the Air Force in May 1970 and trained as a munitions maintenance specialist. His first assignment was at Myrtle Beach Air Force Base (AFB), South Carolina, where he assembled and maintained training munitions for the A-7D. His next assignment was at U-Tapao Air Base (AB), Thailand, where, as a munitions crew chief, he supported the B-52 bombing efforts against North Vietnam, including the Linebacker II operations in December 1972. After a brief stint as a munitions crew chief at Mountain Home AFB, Idaho, he was sent to Kent State University through the auspices of the Airman Education and Commissioning Program to complete a dual-major BA degree in psychology and criminal justice.

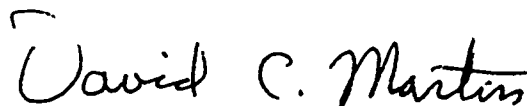
Major Martin was commissioned a second lieutenant after completing Officer Training School in 1975. His first assignment as an officer was at Castle AFB, California, where he performed duties as a Security Police (SP) shift commander. He then was the operations officer for the Security Police squadron at Lajes Field, Azores. Shortly thereafter, he became the Security Police systems and equipment section chief at Headquarters Strategic Air Command, Offutt AFB, Nebraska. He then received an Air Force Institute of Technology assignment to Michigan State University to complete course work for an MS degree in criminal justice. Afterwards, he became the information systems branch chief at the Air Force Office of Security Police (AFOSP), Kirtland AFB, New Mexico, where he was involved in implementing office automation and managing the Air Force standard Security Police automated system. He then became the command-sponsored research fellow from Headquarters AFOSP to the Airpower Research Institute, Maxwell AFB, Alabama. He is currently assigned as the chief of Security Police and squadron commander for the 3380th Security Police Squadron at Keesler AFB, Mississippi.

Major Martin's wife, Mary, is a sociologist, educator, and artist. They have two daughters—Michelle, an architecture student at Ohio State University, and Ann, who will soon enter college as an art student.

Preface

This study began as an effort to write an operational doctrine for Air Force Security Police. When I started my research, I soon discovered that there was no manual on "How to Write an Operational Doctrine" to point me in the right direction. As I set about learning how to write operational doctrine, several points became clear. First, I was going to have to write a "how-to" manual in order to focus the development effort. Second, the doctrine should emphasize air base security since many security activities involve the entire base and not just enforcement personnel. Finally, writing an operational manual for air base security was a long-term project that would require much more work than could be accomplished during a one-year research appointment. Consequently, I spent this year developing and refining my how-to manual as a torch to be passed on to a doctrinal development team that would have the time and resources to develop a comprehensive operational doctrine of air base security. My research is an essential first step toward achieving that goal.

I want to thank the many people who contributed, in one way or another, to my assignment as a command-sponsored research fellow and to my research effort. Without the support of the Air Force chief of Security Police, Brig Gen Frank K. Martin (no, we are not related), together with encouragement from past and present members of the AFOSP staff—Col Fred Miller; Col Dave Southworth; Col Neil Woodcock; Col Tom Johnson, USAF, Retired; and Lt Col Kirk Turner, USAF, Retired—I would not have had the opportunity to take a look at the core of air base security and tell others how I think we should develop an operational doctrine. I also want to thank Col Dennis Drew, the director of the Airpower Research Institute, and recognize the support and helpful inputs of Dr David MacIsaac and Lt Col Manfred Koczur. I particularly want to acknowledge Dr Stephen Blank for keeping me on the right path and Dr Marvin Bassett for helping me organize my writing into intelligible English. Finally, and most important, the continued support of my wife Mary and my daughters Michelle and Ann was essential to my completion of this study.



DAVID C. MARTIN, Major, USAF
Research Fellow
Airpower Research Institute

CHAPTER 1

Why Air Base Security Operational Doctrine?

The Air Force needs an operational doctrine that provides for the security of its forces when they are located on an air base. AFM 1-1, *Basic Aerospace Doctrine of the United States Air Force*, makes only a passing reference to security by advocating "the defense and hardening of forces [together with] active and passive defensive measures and the denial of useful information to an enemy."¹ This study identifies the reasons for writing an operational doctrine and suggests a procedure for developing that doctrine. Further, it evaluates the effect of key environmental factors (e.g., threat levels and the spectrum of conflict) on an operational doctrine based upon traditional security missions.

The Security Police have conducted most of the Air Force's ever-growing and diverse ground-based security missions for over 40 years without the benefit of a formal operational doctrine. Consequently, leaders in this career field have taken a convoluted path toward determining the best way to conduct their missions and have assumed the demanding task of instructing the rest of the Air Force in the application of principles of security. Security Police even had to develop tactical doctrine for an essential defensive security mission—air base ground defense (ABGD)—without consulting an operational doctrine, which forms a bridge between basic doctrine and tactical doctrine. Clearly, the time has come to write an operational doctrine for air base security.

Calls for an Operational Doctrine

Recent changes and/or developments in (1) ABGD doctrinal requirements, (2) readiness reporting, (3) innovation initiatives, and (4) regulatory requirements, underscore the need for an operational doctrine.

ABGD Doctrinal Requirements

On 25 April 1985 the Air Force and the Army entered into a Joint Service Agreement (JSA) for the ground defense of Air Force bases and installations.² This agreement gives responsibility for external ground defense to the Army and internal security to the Air Force. Since the existing Air Force tactical doctrine for ABGD assumes that the Security Police would perform

both internal and external defense, the Air Force must now make significant changes to its ABGD doctrine. The JSA, then, gives the Air Force plenty of impetus to develop an operational doctrine that broadly addresses the ABGD mission (in consonance with applicable Army doctrine) and integrates it with other missions required to fulfill the basic doctrinal goal of security.

Readiness Reporting Study

A staff study conducted by the Air Force Office of Security Police (AFOSP) on the status of resources and training system (SORTS) completed in May 1988 examines the Air Force SORTS as it applies to the ABGD program and Security Police units. The staff study makes some specific recommendations pertaining to ABGD doctrine:

1. Develop and implement an Air Force Air Base Ground Defense doctrine that recognizes and incorporates the facts that air bases are located, in most cases, within a host nation's area of defense responsibility; that in time of general war, air base defensive operations must be conducted in consonance with other U.S. and host nation combat units operating in the vicinity; and that air base ground defense operations must support and contribute to the overall air base operability mission.
2. Develop a strategy that ensures that the doctrine and any subsequent changes are implemented in a planned, deliberate, orderly fashion, timed to coincide with the availability of essential combat equipment and trained forces.³

In essence, the staff study recommends the development of an operational doctrine that supports air base operability.

Innovation Initiatives

In the spring of 1988 the AFOSP chartered an "Innovate in '88" working group to develop innovative ideas for the enhancement of all functional areas within the Security Police career field. The group suggested that a doctrine covering the objectives of the security mission be written for the guidance of the Security Police and the rest of the Air Force.⁴ Other initiatives identified by the group may be pertinent to the first phase in the development of operational doctrine—the collection or information-gathering phase, described later.

Regulatory Requirements

A June 1988 draft revision of AFR 1-2, *Assignment of Responsibilities for Development of Aerospace Doctrine*, tasked the AFOSP with developing base security operational doctrine—AFM 2-XZ.⁵ The AFOSP had already established a position for a command-sponsored research fellowship at the Airpower Research Institute to lay the groundwork for the development of an operational doctrine, in response to suggestions occasioned by the three preceding events.

Defining Operational Doctrine

To begin laying the groundwork for doctrinal development, one must define the phrase *operational doctrine*. A review of pertinent literature (see appendix A) indicates that the Air Force has had difficulty trying to write a clear, functional definition of the term *doctrine*. The following working definition is a synthesis of the attempts found throughout the literature to explain doctrine and its operational subset:

Operational doctrine is an easily understood, broad description of the best way to accomplish functional missions, derived from comparing and contrasting the lessons of recorded operational history, simulations (e.g., exercises, maneuvers, war games), current experience, and applicable principles of war.

Holley's Methodology

The writings of Professor I. B. Holley describe a clear-cut, general methodology for the development of operational doctrine, as defined. His scheme involves three progressive stages: (1) the collection or information-gathering phase, (2) the formulation phase, and (3) the dissemination phase.⁶ AFR 1-2 describes specific procedures for dissemination but leaves all of the procedures for phase 1 and most of those for phase 2 to the discretion of the specific agency developing the doctrine.⁷

An Air Base Security Operational Model

This methodology provides a framework for describing the best way to accomplish the primary missions of air base security within the environmental context of the projected level of threat against aerospace resources (e.g., personnel; equipment; facilities; command, control, and communications; weapon systems; and information). It also addresses the function of those resources within the spectrum of conflict.

Levels of Threat

Several Air Force and Army publications identify levels of threat against aerospace resources. For example, Army Field Manual (FM) 19-1, *Military Police Support for the AirLand Battle*, categorizes them by size and composition, methods and missions, likely targets, probable weapons and equipment, and expected area of operation.⁸ These descriptions apply to customary wartime threats occurring in the rear battle area—primarily in the European theater—but ignore criminal acts directed against military resources during the Korean conflict and Vietnam and in current situations throughout the world. FM 19-1 also ignores low-level threats to targets such as information systems. Army Pamphlet 525-14/Air Force Pamphlet 206-4, *Joint Operational Concept for Air Base Ground Defense*, describes

three levels of threat to an air base: (I) the threat from agents, saboteurs, partisans, and terrorist groups; (II) the threat from tactical units smaller than battalion size, particularly forces trained in unconventional warfare (e.g., Spetsnaz and ranger-commandos), whose primary tasks are covert reconnaissance and sabotage missions to disrupt friendly sortie generation; and (III) the threat from tactical military units of battalion size or larger, engaged in heliborne, airborne, amphibious, or ground-force operations.⁹

Spectrum of Conflict

Speculation about the number of elements in the spectrum of conflict is as diverse as the definitions of the term *doctrine*. The low end of the spectrum might include individual or group actions designed to achieve extremely limited political, military, or economic objectives (e.g., robbing an Air Force accounting and finance office, bombing an aircraft, or taking hostages at the base hospital). One moves across the spectrum from this limited level of conflict through military coups, insurgency, low-intensity peacekeeping and peacetime contingency operations, midintensity conventional warfare, high-intensity conventional warfare, theater nuclear warfare, toward strategic nuclear and postnuclear warfare—the high end of the spectrum.¹⁰ These levels are not discrete, are nominal at best, sometimes tend to overlap, and may occur simultaneously at different locations around the globe.

Current Missions

Without the benefit of a formal doctrine, Air Force Security Police have developed a variety of missions over the past 40 years or have adopted some from the Army provost marshal and from military police heritage. These missions, formed to counter various levels of threat over the entire spectrum of conflict, have been legitimized by Air Force regulations and manuals but are not rooted in any explicit doctrine, with the exception of ABGD tactical doctrine. Each of the four primary mission areas (system security, information security, law enforcement, and air base ground defense) has evolved into a series of subfunctions—40 altogether—that are now generally performed by Security Police and by other Air Force personnel.

Tieing It Together

Writing a proper operational doctrine for air base security is heavily dependent upon the convergence of environment and mission. By pairing the environmental factors (i.e., the levels of threat and the elements within the spectrum of conflict), we generate a number of combinations, each representing a possible scenario to which security forces might have to respond. We must then make a selection from established security missions that would provide an appropriate response to the particular scenario. For scenarios for which there is no precedent (e.g., a level II threat encountered during strategic nuclear warfare), we would have to develop

theoretical missions to meet those challenges. In short, by applying a reasonable methodology to a realistic data base, we can develop an operational doctrine that addresses the needs of Air Force security.

Notes

1. AFM 1-1, *Basic Aerospace Doctrine of the United States Air Force*, 16 March 1984, 2-6 through 2-7.
2. Department of the Army Pamphlet (DAP) 525-14/Air Force Pamphlet (AFP) 206-4, *Joint Operational Concept for Air Base Ground Defense*, July 1986, 3.
3. Air Force Office of Security Police (AFOSP), "SORTS Staff Study Report," May 1988, 10.
4. Report of AFOSP Innovation Staff Study Group, "Innovate in '88," April 1988, 2, 4, 17.
5. AFR 1-2, "Assignment of Responsibilities for Development of Aerospace Doctrine," June 1988 (draft), 18.
6. I. B. Holley, "The Doctrinal Process: Some Suggested Steps," *Military Review* 59, no. 4 (April 1979): 2-13.
7. AFR 1-2, 32-33.
8. Army Field Manual (FM) 19-1, *Military Police Support for the AirLand Battle*, December 1983, 2-3 through 2-4.
9. DAP 525-14/AFP 206-4, 4.
10. Lt Col David J. Dean, *The Air Force Role in Low-Intensity Conflict* (Maxwell AFB, Ala.: Air University Press, 1986), 3, 5-6.

CHAPTER 2

Levels of Threat

One essential goal of air base security doctrine should be to counter the threats against a base's resources and personnel. We must identify the levels of threat that are currently focused against Air Force resources and personnel before we can develop the proper doctrine for countering those forces. Once we identify the levels of threat, we can then gather historical and theoretical data on the best ways to handle them. Defining the types of threats—basic and levels I, II, and III, mentioned previously—is a key step in creating the proposed three-dimensional model for air base security operational doctrine. It is especially important to examine the basic threats encountered daily at an Air Force installation because of their frequency of occurrence, at least in peacetime (although they can occur throughout the entire spectrum of conflict).

Lowering the Threshold: Basic Threats

Experience has shown that property crimes, crimes against persons, traffic accidents, drug offenses, protests, and riots are basic threats that occur both during peace and war. The threat to resources and personnel not addressed by levels I, II, and III can have as serious an impact on mission capability as sabotage or engagement with enemy forces. At the conclusion of the Korean War, the Far East Air Forces determined that Korean nationals employed at its bases removed enough government resources to cause more economic loss to the Air Force than did North Koreans and the Chinese. The threat of theft against US resources in the Korean conflict was more serious monetarily than any of the level I or II threats that occurred: "Not a single Air Force installation was attacked by guerilla soldiers or saboteurs. No aircraft were lost or even damaged due to sabotage."¹ Although some people may argue that level I agents or sympathizers stole funds and equipment for the North Koreans, no data supports this supposition. Certainly, the levels of threat are not always discrete or mutually exclusive, and some overlap may take place. The essential point, however, is that such basic threats exist and must be considered important environmental factors in an operational doctrine for air base security.

The Air Force crime statistics for 1987 reflect the scope of this basic threat. Of the 139,752 incidents reported that year, 17,429 were crimes against persons and 55,530 were property crimes. In addition, 20,766

on-base traffic accidents were reported, including 25 deaths associated with 20 of those accidents. Finally, 2,917 drug offenses occurred during the year.² All of these incidents posed direct or indirect threats to Air Force personnel or resources.

Theft may be the work of individuals, small groups, or organized criminals, any of whom may be rank amateurs or professionals. Their methods and actions are highly variable, depending upon the size and value of the target, existing security, time of day, ease of access, and a host of other factors. They may conduct surveillance of their targets, get information from inside sources, or simply break in, hoping to find something of value (targets of opportunity) that can be sold, traded, or retained for personal use. Probable weapons and equipment include handguns, knives, burglar tools, and explosives, while areas of operation include flight lines, warehouses, and maintenance areas on air bases as well as remote, unmanned Air Force sites that support air bases.

Robbers, acting alone or in small groups, typically move rapidly and forcefully against their targets—usually sources of cash on an air base. They use handguns, shotguns, rifles, knives, and often some type of getaway vehicle in robberies of accounting and finance offices, property disposal yards, base exchanges, commissaries, and other locations where government funds might be located on an air base.

Use of illegal drugs is a direct threat to Air Force personnel and an indirect threat to air base resources controlled by people under their influence. Drug users, acting individually or collectively, may damage or destroy Air Force resources because their altered mental state can lead to serious errors in judgment. Further, these people—who could be located anywhere on base—might be armed with handguns or knives and thereby increase their threat to Air Force personnel.

Protestors and rioters present threats that vary from minimal blockage of essential lines of communications to major violence and destruction of air base resources. Operating individually or in groups of various sizes, they engage in active or passive protests or riots directed against air base entry points, military convoys, or key on-base locations and may use rocks, clubs, firebombs, Mace, helmets, gas masks, body armor, and shields.

Domestic violence, typically initiated by verbal disputes, occurs frequently on air bases and often leads to injury or death. It may involve husband and wife, siblings, roommates, supervisor and subordinate, or other people. Police respond warily to these incidents because of the potential for danger inherent in the emotional and irrational actions of the parties involved. Although domestic violence may take place anywhere on the air base, it usually occurs in base housing, barracks, clubs, or billeting areas.

Traffic accidents can injure or kill Air Force personnel, damage or destroy Air Force vehicles, and impair key lines of communications (roads, flight lines, marshaling areas, and so on). Although they are not intentional threats directed at specific targets, traffic accidents are destructive and disruptive, nevertheless.

Because air base security must deal with these basic threats daily, they should be considered in any development of operational doctrine, particularly since they present an obvious, visible risk to air base personnel, funds, and physical resources. Such doctrine must also evaluate more traditional threats to military activities and air bases.

Level I Threats

Enemy espionage agents, popularized by books and movies, are an established threat to air bases. Acting individually or in small cells as part of an organized network, they conduct clandestine surveillance, sabotage, and subversion, and gather intelligence about air base operations and defenses including nuclear and/or chemical weapons and delivery systems, radar, air defense, communications sites, and logistical centers. Agents also support level II special-purpose forces (e.g., Spetsnaz and ranger-commandos) and use weapons and equipment ranging from simple burglar tools to sophisticated cameras and listening devices, long-range secure radios, silenced automatic weapons, sniper rifles, and explosives.*

Terrorists, the most visible of the level I threats, are specially trained individuals or small groups able to operate with military precision and exploit vulnerabilities through the use of violence, speed, and surprise. Armed with automatic pistols, assault rifles, rocket-propelled grenade launchers, small explosives, hand-held and other radios, they conduct sabotage, steal military supplies and equipment, and attack civilians, together with US and host-nation military officials and their families (2-3).

Enemy sympathizers are the least prominent of the level I threats because their activities are often attributed to agents and/or terrorists. Sometimes recruited by level I agents, they act alone or with other sympathizers, attacking random targets of opportunity. They use small automatic weapons and explosives that are bought, stolen, homemade, or supplied by level I agents in their strikes on convoys, communications lines, public utilities, and remote radar/communications sites (2-3). Because sympathizers are usually amateurs, they avoid well-protected targets that are beyond their means to attack successfully.

Level II Threats

The threat to air bases by special-purpose forces such as the Soviet Spetsnaz and the North Korean ranger-commandos is widely discussed within Air Force circles. These forces are usually the size of a squad or smaller but may be as large as a platoon or company, and dress in host-nation uniforms, civilian clothes, or their standard airborne uniform.

*Army Field Manual 19-1, *Military Police Support for the AirLand Battle*, December 1983, 2-3. Subsequent page references to FM 19-1 are cited parenthetically in the text.

Manned with skilled officers and senior noncommissioned officers (NCOs) who are highly trained in demolitions, burglaries, communications, and languages, they deploy by parachute, helicopter, vehicle, on foot, or by boat. These forces collect intelligence; perform reconnaissance and sabotage; mislead, disrupt, or destroy enemy forces; and prepare for incursions by larger forces (level III threat). Carrying a full complement of explosives, incendiary devices, and possibly nuclear, chemical, and/or biological (NBC) weapons in addition to long-range secure radios, hand-held antitank weapons, antiaircraft weapons, and automatic weapons with flash suppressors and silencers, they attack nuclear weapons storage sites and launch systems, command posts, air defense systems, communications sites, convoys, prepositioned war stocks, and reserve units (2-3).

Long-range reconnaissance units, consisting of specially selected and trained five-man teams deployed by airdrop or infiltration, create a similar threat. By means of observation, ambush, raid, and interrogation, they conduct reconnaissance for avenues of approach into the rear areas where most air bases are located. Using explosives, incendiary devices, assault rifles, antitank grenade launchers, light machine guns, and secure radios, these teams concentrate on nuclear delivery systems; command, control, and communications (C³) facilities; radar sites; troop locations; and logistics movements. Division-level teams operate up to 100 kilometers (km) from the forward edge of the battle area (FEBA), and army-level teams up to 350 km from the FEBA (2-3).

Troop reconnaissance groups—deployed in scout reconnaissance vehicles, in infantry-fighting vehicles, in medium tanks, and on motorcycles—pose an even greater threat. Traveling on existing roads until contact is made or expected with enemy forces, they conduct ground reconnaissance for avenues of approach to rear areas. Armed with antitank grenade launchers, assault rifles, antitank guided missiles, portable surface-to-air missiles (SAMs), light machine guns, 125-millimeter (mm) guns, 73-mm guns, 14.5- and 7.62-mm machine guns, they concentrate on nuclear weapons and delivery means, defensive positions, command headquarters, and communications centers. These reconnaissance groups can operate on a width of 50 to 60 km, up to 50 km from the FEBA in a conventional conflict, and 50 to 100 km in a nuclear environment (2-3).

Level III Threats

Airmobile forces, ranging in size from a company to a reinforced battalion, are a major threat to an air base, as are all level III threats. These forces are inserted by helicopter to destroy nuclear weapon storage sites and launch systems, major logistical facilities, and other rear-area targets such as nuclear weapon storage and launch systems, command and control headquarters, major logistical clusters, early warning systems, key terrain, airfields, reserve forces, and avenues of approach to the rear area. In

addition to seizing key terrain and exploiting the results of tactical air operations or penetrations, they also conduct deception operations. Airmobile forces operate up to 50 km from the FEBA and are furnished with assault rifles, heavy and/or light machine guns, antitank grenade launchers, antitank guided missiles, SAMs, mortars, wheeled scout reconnaissance vehicles, automatic grenade launchers, recoilless guns, antitank guns, self-propelled antiaircraft guns, tracked infantry-fighting vehicles, and equipment for tactical air support (2-4).

Amphibious forces the size of a platoon or regiment, consisting of elite naval infantry (marine) units—much like motorized rifle units—are a major threat to air bases located close to coastal areas or large rivers. Operating alone or with ground forces, they deploy by ship or amphibious craft to perform commando-type raids, reconnaissance, and sabotage missions. These forces use weapons and equipment similar to those of airmobile forces to seize key coastal and island positions to create diversions, inflict damage near the coast, flank enemy forces, conduct reconnaissance, report targets of naval significance, and help ground and naval units destroy the enemy. Likely targets include air bases, ports, and other key objectives (2-4).

Airborne forces of company to division size are elite parachute divisions, deployed by fixed-wing aircraft and/or helicopters, which attempt to encircle enemy forces, destroy nuclear delivery systems, and seize key terrain, airheads, and river-crossing sites. They exploit weak areas and conduct strategic assaults against air bases, bridgeheads, landing zones, drop zones, and command and control headquarters. Using weapons and equipment similar to those of airmobile and amphibious forces, the airborne forces perform tactical assaults up to 100 km from the FEBA, operational assaults up to 300 km from the FEBA, and strategic assaults up to 1,000 km from the FEBA (2-4). Air bases can be found in any of these areas.

Ground infiltration forces are composed of individuals and small groups that later form into elements of company or battalion size. In difficult terrain and/or lightly defended areas, they infiltrate singly or in small groups by foot, inland waterway, or open sea, transiting long distances and then forming into units. Armed with automatic pistols, assault rifles, light machine guns, antitank grenade launchers, antitank guided munitions, SAMs, and explosives, these forces operate deep in the rear area with the intent to destroy or disrupt the following targets without becoming decisively engaged: nuclear weapon storage sites and delivery systems, troop concentrations, logistics lines of communications, and convoys—any or all of which can be associated with air bases (2-4).

Ground-penetration forces are company to battalion size and are found in first-echelon motorized rifle or tank divisions. They attempt to penetrate the main battle area and attack targets in the rear area such as command and control facilities, prepositioned war stocks, defense positions, reserves, and rear-area forces found on air bases. Their weapons and equipment include assault rifles, heavy and/or light machine guns, antitank grenade launchers, antitank guided munitions, SAMs, mortars, wheeled scout

reconnaissance vehicles, recoilless guns, self-propelled antiaircraft guns, amphibious armored personnel carriers, tracked infantry-fighting vehicles, and medium tanks (2-4).

Operational maneuver groups range in size from one to several divisions and are generally reinforced by airborne or airmobile forces. Committed by front or army before the first-echelon battle ends and before second-echelon forces are committed, these groups are deployed as a tank-heavy operational raid force that attacks at high speed on a separate axis to strike intermediate targets without becoming decisively engaged. In addition to weapons and equipment similar to those of ground-penetration forces, they use self-propelled multiple rocket launchers, self-propelled and towed artillery, tracked infantry-fighting vehicles, amphibious armored personnel carriers, medium tanks, attack and/or support helicopters, and tactical air support equipment. These weapons and equipment are directed against politically and/or economically significant centers, large rear-area targets, nuclear weapons, reserves, airfields, C³ facilities, and withdrawing troops (2-4).

These threats comprise the first dimension of our model of an operational doctrine. Because existing threats may vary considerably from these generic descriptions, an operational doctrine should be flexible enough to allow for such variances. When planners use operational doctrine to develop new strategies and policies, they should also examine current intelligence on specific existing threats. Because air base security personnel operate in a frequently changing environment of threat and conflict, we must understand the other half of that environment—the spectrum of conflict—in order to develop a useful and practical operational doctrine.

Notes

1. Roger P. Fox. *Air Base Defense in the Republic of Vietnam, 1961-1973* (Washington, D.C.: Government Printing Office, 1979), 6.
2. *Security Police Digest*, October 1988, 1.

CHAPTER 3

Spectrum of Conflict

Just as we must appreciate the importance of levels of threat to the operational environment of air base security, so must we realize that an understanding of the spectrum of conflict is essential in developing an operational doctrine. On the one hand, air power and the bases that support it play little if any role in some areas of the conflict spectrum. On the other hand, air power is important and air base security operations are essential to other portions of the spectrum. Understanding the significance of the entire spectrum of conflict to the military operational environment is commendable, but this chapter confines itself primarily to the elements of the spectrum that involve air base security operations.

Contemporary military literature uses the phrase *spectrum of conflict* in referring to the range of violence that can occur between opposing forces. The lower level of violence is called low-intensity conflict (LIC) and, according to the US Air Force and Army, includes (1) insurgency and/or counterinsurgency activities, (2) counterterrorism and antiterrorism activities, (3) peacekeeping operations, and (4) peacetime contingency operations.¹ Midintensity conflict ranges from limited to major conventional warfare, while high-intensity conflict extends from limited to major nuclear warfare.²

The conflict spectrum is a relative concept, particularly in terms of its level of violence. For example, the side on the receiving end of the violence in a low-intensity conflict would likely view the level of intensity as rather high, especially when people are being killed. Some authorities have attempted to strengthen or add depth to the definition of spectrum of conflict by incorporating the probability of occurrence. Thus, low-intensity conflicts have a relatively high probability of occurrence, whereas that probability decreases as one moves across the spectrum toward midintensity and high-intensity conflicts. Consequently, major global nuclear war is seen as having the lowest probability of occurrence.

Current definitions of the spectrum of conflict do not address some of the conflicts that air base security forces deal with frequently—almost daily at some air base locations. These conflicts generally take place as a result of the security force encountering one of the basic threats described in chapter 2. They fit in the spectrum by virtue of the involvement of military forces (usually Security Police) in low-violence situations having a high probability of occurrence. Again, the level of violence is a relative term since Security Police or members of the opposing side may be and have been killed during these conflicts.

Air base operations do not take place uniformly throughout the spectrum of conflict, particularly in some low-intensity-conflict activities (e.g., those involving internal defense and development—IDAD—normally conducted by the US Army). Consequently, this review of the spectrum focuses upon conflicts that require air base security and for which operational doctrine can be developed.

Spreading the Range: Primary Conflicts

Air base security forces may find themselves in altercations with one to several individuals who pose some level of threat occurring below the realm of a traditional low-intensity conflict. Indeed, Security Police put their lives at risk daily and are sometimes killed when the violence intensifies (e.g., during an armed robbery or the taking of hostages).

Primary Criminal Conflicts

A primary criminal conflict occurs when an air base security force (usually Security Police law enforcement specialists) takes action against a basic criminal threat. Such conflicts include a patrol responding to an armed robbery or stopping an intoxicated driver, the apprehension of a criminal suspect, and emergency-service-team operations in a hostage situation. These types of activities take place frequently enough that specific air base security missions have been developed to respond to the threats and resolve the conflict (chapter 4 addresses each of these missions). One factor common to primary criminal conflicts is that a specific law, military regulation, or article of the Uniform Code of Military Justice (UCMJ) has been violated.

Primary Domestic Conflicts

Primary domestic conflicts involve air base security responses to such basic threats as public protests, potential riots, or instances of domestic violence. They are distinguished from primary criminal conflicts in that although a law, regulation, or article of the UCMJ has not been violated, a strong potential for violation exists.

Low-Intensity Conflicts

Joint Chiefs of Staff (JCS) Publication 1, *Department of Defense Dictionary of Military and Associated Terms*, contains a definition of low-intensity conflict:

A limited politico-military struggle to achieve political, social, economic, or psychological objectives. It is often protracted and ranges from diplomatic, economic, and psychosocial pressures through terrorism and insurgency. Low-intensity conflict is

generally confined to a geographic area and is often characterized by constraints on the weaponry, tactics, and the level of violence.³

The Army and Air Force—in their final draft of Army Field Manual 100-20/Air Force Manual 2-XY, "Military Operations in Low-Intensity Conflict"—provide the following LIC definition for operational doctrine:

Low-intensity conflict is a politico-military confrontation between contending states or groups below conventional war and above the routine, peaceful competition among states. It frequently involves protracted struggles of competing principles and ideology. Low-intensity conflict ranges from subversion to the use of armed force. It is waged by a combination of means, employing political, economic, informational, and military instruments. Low-intensity conflicts are often localized, generally in the Third World, but contain regional and global security implications.⁴

One or more of the four military operations associated with low-intensity conflict—insurgency/counterinsurgency, counterterrorism and antiterrorism activities, peacekeeping operations, and peacetime contingency operations—may take place at any one time and may have an impact on air base security operations.

Insurgency/Counterinsurgency

Insurgency operations involve air base support for a revolution—generally in a third-world nation—while counterinsurgency activities are essentially counterrevolutionary. These actions may include special operations and internal defense and development.⁵

Special Operations. Special operations in support of or opposed to revolutions usually do not take place on US Air Force bases. Rather, the aircraft, personnel, and resources used to conduct these activities are located either on permanent or temporary air bases specifically designed to support special operations. Basic, level I, and level II threats could create conflicts for air base security during these operations. Examples of air base security operations occurring within this portion of the spectrum of conflict include capturing an espionage agent attempting to obtain special operations plans, using explosive-detector dogs to locate terrorist bombs, and using air base ground defense forces to block an attempted air base attack by revolutionary special-purpose forces.

Internal Defense and Development. IDAD functions such as balanced development, security, neutralization, and mobilization utilize air power for transportation, resupply, and close air support (CAS).⁶ When US Air Force air power and air bases are involved, the conflicts confronted by air base security are essentially the same as those encountered during special operations.

Counterterrorism and Antiterrorism

The United States views all terrorist acts as criminal, regardless of whether or not a state of war exists. During peacetime, terrorism constitutes a violation of laws, regulations, and the Uniform Code of Military Justice—much like primary criminal conflicts. During wartime, terrorism

is a violation of the Geneva Conventions and, therefore, a war crime. Examples of air base security conflicts involving terrorism (a-level I threat) include exchanging weapons fire with a terrorist group attempting to attack a key air base resource, using an explosive-detector dog to discover terrorist bombs, and thwarting a terrorist attempt to take the base commander hostage.

Peacekeeping Operations

Peacekeeping operations include (1) withdrawal and disengagement, (2) cease-fires, (3) prisoner of war exchanges, (4) arms control, and (5) demilitarization/demobilization.⁷ Because US Air Force air bases would generally support these operations, security forces would face attendant conflicts involving basic or level I threats similar to those mentioned earlier.

Peacetime Contingency Operations

Peacetime contingency operations include (1) disaster relief, (2) shows of force/demonstrations, (3) noncombatant evacuation operations, (4) rescue and recovery operations, (5) strikes and raids, (6) peacemaking, (7) unconventional war, (8) security assistance surges, and (9) support to US civil authorities.⁸ Air base security could be heavily involved in many of these operations and, in the process, might encounter conflicts created by basic and level I or II threats.

Midintensity Conflicts: Conventional Warfare

Conventional warfare—whether limited or unlimited—distinguishes midintensity conflicts.⁹ Typically, air base security would be engaged in full-time war operations and could expect conflicts arising from basic or level I, II, or III threats. These conflicts could include everything from catching a foreign-national base employee stealing mission-essential aircraft parts to exchanging weapons fire with a Soviet ground-penetration company attempting to capture the base.

High-Intensity Conflicts: Nuclear Warfare

High-intensity conflicts entail limited or unlimited nuclear warfare.¹⁰ Providing that the air base has survived the initial nuclear strike and is conducting air power operations, security personnel can expect to encounter the same threats and conflicts that occur in midintensity scenarios. Furthermore, the postnuclear environment (e.g., civilians looking for food or sanctuary) will probably make air base security operations more difficult by confronting security forces with moral dilemmas.

Thus, the spectrum of conflict presents challenges that operational doctrine must address. Although specific air base security missions—the third element in our doctrinal model—have yet to be established for some types of conflicts, a number of missions are already in place. Collectively, these missions address the entire scope of air base security.

Notes

1. Army Field Manual (FM) 100-20/Air Force Manual (AFM) 2-XY, "Military Operations in Low-Intensity Conflict," July 1988 (final draft), 1-13.
2. Sam C. Sarkesian, "The Myth of US Capability in Unconventional Conflicts," *Military Review* 68, no. 9 (September 1988): 8, 11.
3. Joint Chiefs of Staff (JCS) Publication 1, *Department of Defense Dictionary of Military and Associated Terms*, 1 June 1987, 214-15.
4. FM 100-20/AFM 2-XY, 1-1 through 1-2.
5. *Ibid.*, 2-34 through 2-41.
6. *Ibid.*, E-4.
7. *Ibid.*, 4-1.
8. *Ibid.*, 5-7.
9. Sarkesian, 8, 11.
10. *Ibid.*

CHAPTER 4

Current Missions

The primary areas of air base security—law enforcement, systems security, air base ground defense, and information security—comprise the final element of the model for operational doctrine. These missions were developed, primarily by Security Police, to ensure optimum air base security during all levels of threat throughout the spectrum of conflict. A broad description of the operational tasks associated with each mission area clarifies their function within the context of air base security.

Law Enforcement

The law enforcement mission and tasks have been developed to protect air base personnel and some resources (other resources are protected by systems- and information-security missions), to maintain law and order, to enforce regulations and the Uniform Code of Military Justice, and to provide associated services. These activities were designed to counter all basic threats, some level I threats, primary conflicts, and low-intensity conflicts.

Operations

Law enforcement operations are customarily the most visible air base security activities at any Air Force installation. They run the gamut from controlling entry to the air base and directing traffic flow to apprehending suspects and handling protestors.

Command, Control, and Communications. Command, control, and communications (C³) for law enforcement operations originate with the law enforcement desk, which monitors activities and intrusion detection systems (IDS), directs responses, notifies key personnel when appropriate, and keeps a record of events. The law enforcement desk, when notified of an impending or ongoing threat or conflict, directs the activities necessary to resolve the situation. Command and control orders from higher authority are routed through the desk to law enforcement personnel who respond to the threat or situation. This point of control is the hub for most day-to-day law enforcement activities.

Resource Protection. Air base personnel responsible for government property perform resource protection activities designed to secure air base resources against basic and level I threats such as thieves, robbers, enemy agents, and terrorists. Examples of this protection include the use of safes,

IDS, and locked warehouses, together with controlling access to air base assets by means of manned or automated checkpoints and identification procedures.

Installation Patrol. Security Police personnel and military working dogs patrol an installation to detect basic or level I threats and engage in the primary and/or low-intensity conflicts that generally result when a threat is detected. Other responsibilities include crime deterrence, traffic control, and resource protection.

Installation Entry Control. Security Police control access to an air base by allowing only authorized personnel to enter. This screening procedure thus protects the installation against basic and level I threats. The control points also monitor personnel exiting the air base and can block the escape of people who have initiated primary or low-intensity conflicts.

Detention. Most Security Police organizations have facilities for temporarily detaining suspects apprehended on an air base and/or for holding them in pretrial confinement. Long-term detention, however, is reserved for large correctional facilities not usually located on base. During mid-intensity or high-intensity conflicts in wartime, security forces may also hold prisoners of war prior to their relocation to POW camps.

Investigation. Investigation functions conducted by Security Police or agents from the Office of Special Investigations (OSI) confirm that a conflict has occurred and identify the individuals responsible. If this procedure is successful, the culprits are then processed through the military or civilian criminal justice system, thereby reducing the air base threat by removing its source.

Military Working Dogs. Military working dogs, trained for installation patrols, track criminal or terrorist suspects from the scene of the conflict and identify the locations of terrorist bombs and illegal drugs. These animals are also excellent deterrents to potential riots and other violent conflicts.

Emergency Services Teams. Emergency services teams consist of individuals with specialized skills and training who resolve conflicts involving armed criminals or terrorists. The criminals/terrorists have typically barricaded themselves and/or taken hostages, thus posing a threat to air base personnel and resources.

Protest/Riot Control. Large numbers of air base Security Police and other personnel prevent protestors and/or rioters from damaging, destroying, or illegally controlling installation resources, lines of communications, and/or property. This type of conflict is infrequent and dependent on the political climate in the country where the air base is located.

Admin'stration and Reports

Supervision of reports and analyses, passes and registration, and administrative security activities supports air base security and helps counter basic and level I threats.

Reports and Analyses. Some law enforcement personnel process reports on primary and low-intensity conflicts used in adjudicating cases involving people suspected of such activities. Air base security personnel analyze these reports to detect trends in both primary and low-intensity conflicts, thereby assisting law enforcement forces in anticipating times, locations, and types of threats/conflicts that may reoccur.

Pass and Registration. By processing, preparing, issuing, and controlling various forms of identification as well as registering vehicles and firearms, personnel who conduct these procedures supplement other ways of limiting access to the air base and restricted areas.

Information Security Administration. The law enforcement mission includes people who manage, inspect, and supervise the variety of programs and tasks peculiar to information security.

Systems Security

Security Police assist owners and/or users of operational resources such as aircraft; missiles; nuclear weapons; and command, control, and/or warning systems in protecting these resources against basic, level I, and some level II threats encountered throughout the spectrum of conflict.

Command, Control, and Communications

System security command, control, and communications are handled separately from law enforcement C³, and at a different location on base. Once referred to as central security control, this system security C³ center is now known as close-defense area headquarters.¹ Aside from the type of air base forces controlled by this center—security specialists rather than law enforcement specialists—its functions are similar to those of the law enforcement desk.

Priority Resource Security

A system of priorities determines how security forces and resources are allocated to protect Air Force operational assets. Delivery systems for nuclear weapons, the weapons themselves, and certain C³ functions have the highest priority and are kept in restricted areas that provide physical protection, intrusion detection systems, sentries, patrols, and response units. Other assets have lesser priorities reflecting their function, alert status, maintenance status, and other factors.

Aircraft. Alert aircraft armed with nuclear weapons have the highest security priority, based upon anticipated or actual threats of at least level I status. Their aircrews are similarly protected within restricted areas. Nonnuclear alert aircraft for air defense, bombing, refueling, airborne warning and control, and specialized functions have slightly lower

priorities. Operational aircraft not on alert have a still lower priority but require some security to counter threats.

Missiles. Intercontinental ballistic missile (ICBM) systems on alert have a high priority for protection since they are equipped with nuclear warheads and are a primary deterrent against nuclear war. The missiles and their launch crews are secured in hardened structures with intrusion detection systems and dedicated security forces designed to counter all levels of threat throughout the spectrum of conflict. Air base forces responsible for missile security face unique problems since the weapons are located in remote areas and are separated from each other and the air base by long distances.

Nuclear Weapons. Nuclear weapons have a high security priority, no matter their function or location. Dedicated security forces protect them against all threat levels throughout the spectrum of conflict.

Command, Control, Communications, and Warning. The type of protection provided to command, control, communications, and warning systems depends upon the security priority of the operational assets they support. Because these systems are not always located on base, they may be assigned dedicated security patrols and/or special response teams.

Air Base Ground Defense

The air base ground defense mission—including command, control, communications, and intelligence (C³I); internal defense; and external defense operations—protects overseas bases during conflicts of at least low-intensity status. ABGD counters level I and II threats and delays or disrupts level III threats, pending the arrival of US Army and/or host-nation tactical defense forces. Although not generally a part of peacetime air base security operations, ABGD mission tasks are taught to security forces and frequently exercised. Systems security forces are organized as squads and fire teams that can transition into ABGD operations when required.

Command, Control, Communications, and Intelligence

A base defense operations center (BDOC) is responsible for C³I during ABGD operations. The BDOC exists to “plan, direct, coordinate, integrate, and control the efforts of all the organic and attached ABGD assets as well as those non-organic US Army, host nation, or allied assets placed under the operational control of the ABGD force commander.”² Essentially, the BDOC oversees internal and external ground defense operations against actual and impending level I, II, or III threats at any point in the spectrum of conflict.

Internal Defense

Security Police forces and base augmentation personnel use patrols, observation posts, obstacles, sensors, and area-denial munitions to defend

the air base against all levels of threat.³ These internal defense operations are coordinated and integrated with those of the external defense mission through the BDOC.

External Defense

A recent change to the external security mission of air base ground defense assigns responsibility for external defense to US Army military police and/or host-nation military personnel.⁴ Joint doctrine is currently being developed to address this aspect of the ABGD mission.

Information Security

The purpose of the information security mission is to protect classified information and ensure that base personnel who have access to this material are trustworthy. Some of these security activities are managed, inspected, and/or supervised by administrators who work in law enforcement, while other activities, such as communications and computer security, are managed by functional specialists. Traditionally, information security counters basic and level I threats throughout the spectrum of conflict, although most forms of classified information are also protected against level II and III threats.

Information Security Program

An information security program implements Department of Defense and Air Force regulations concerning the protection of classified information from basic and level I threats by reporting and investigating program violations.

Personnel Security Program

A personnel security program performs background investigations before granting security clearances to people who require access to classified information and restricted areas. The program thus screens out individuals who may pose a basic or level I threat to air base information and resources.

Industrial Security Program

Protecting classified information that must be provided to defense contractors working at an air base is the province of the industrial security program. Security Police usually supervise the program and perform the required inspections.

Classification Management

A classification management program assigns to official information a level of classification that reflects the relative importance of that information. The level of classification, which determines how the information

security program will protect the classified material, is generally made by the originator of the information or is derived from other classified documents.

Security Education Program

The security education program reinforces other information security programs by ensuring that all people who have access to classified information and/or restricted areas are aware of proper security procedures.

Wartime Information Security Program

Specialized activities of the wartime information security program protect classified information when the United States is at war. Consequently, the program is implemented during midintensity and/or high-intensity conflicts.

Computer Security

Computer security (COMPUSEC) applies the principles of the information security program to the processing, storage, utilization, production, and transmittal of classified information within and between computers and other devices designed to store classified information, such as memory typewriters. This program uses hardware, software, and standard Air Force physical security measures (e.g., locked storage, limited access, and IDS) to protect classified information from potential or known threats—predominantly basic and level I.

Communications Security

Communications security (COMSEC), a program for protecting the transmittal or reception of classified information over various air base communications systems, counters attempts at hostile collection by basic or level I threats. Using secure telephones rather than "talking around" classified information over an unsecure phone is one example of the program's security measures.

Operations Security

Operations security (OPSEC) is used in conjunction with other information security programs to protect air base operations from level I threats of enemy intelligence collection. OPSEC measures include limiting the public release or discussion of unclassified information that, when collated and combined with other data gathered by enemy intelligence, may reveal classified plans or operations.

These air base security missions were developed to counter various environmental factors (i.e., specific threat levels over the spectrum of conflict). By matching the missions against a permutation of environmental

factors, we create a multidimensional model that can be used in developing an operational doctrine for air base security.

Notes

1. AFR 207-1, *The Air Force Physical Security Program*, October 1988, 6-1.
2. AFR 206-2, *Air Base Ground Defense*, 22 September 1983, 34.
3. Department of the Army Pamphlet (DAP) 525-14/AFP 206-4, *Joint Operational Concept for Air Base Ground Defense*, July 1986, 5.
4. Ibid.

CHAPTER 5

A Recommended Process of Doctrinal Development

Chapters 2-4 examined the air base environment (threats and conflicts) and the traditional missions that were developed to achieve security within that environment. We can now use this operational model of the current state of air base security in conjunction with an approach to doctrinal development recommended by Professor I. B. Holley, Jr.

Professor Holley and the Writing of Doctrine

Professor Holley provides a structured, systematic methodology that can be used in writing a utilitarian doctrine of air base security for the Air Force. Holley cautions that some efforts to write military doctrine have used the terms *concepts* and *principles* interchangeably with *doctrine*¹ and believes that failure to differentiate among the three terms can lead to a lack of precision and uniformity.² He emphasizes that *concepts* are unofficial, tentative inferences or hypotheses derived from observations, whereas *principles* are "self-evident truths" derived by "abstractions through heuristic analysis of individual instances."³ *Doctrine*, on the other hand, comprises officially authenticated generalizations established by a thorough analysis of a large sampling of military experiences.⁴ These generalizations are the result of compiling a wide range of recorded experiences that provide insight into the proposed doctrine. Holley refers to this activity as the collection phase.*

Following the collection phase is an analysis or formulation phase that sifts through the collected experiences and identifies those that produce optimum results—the best ways of getting the job done (8-9). Of course, the strength of this process of generalization depends on the quality of the supporting evidence.

Last, the dissemination phase refines, reviews, and sanctions these generalizations (10-11). Thus, operational doctrine is the official statement of the best way to accomplish a particular military objective, such as air base security. These three phases—collection, formulation, and dissemination—provide an orderly, building-block approach to writing doctrine.

*Maj Gen I. B. Holley, Jr., "The Doctrinal Process: Some Suggested Steps," *Military Review* 59, no. 4 (April 1979): 5. Subsequent page references to this article are cited parenthetically in the text.

Phase 1: Collection

The collection phase gathers relevant experiences from a variety of sources such as (1) the recorded combat experience of the US military, (2) the recorded combat experience of other countries, (3) full-scale maneuvers, (4) unit exercises/service tests, (5) war games/command-post exercises, (6) systematic and continuous bibliographic searches, and (7) liaison with other internal and external agencies (5-8).

US Combat Experience. Although the recorded combat experience of US military personnel and observers is a primary source of information, Holley cautions that "merely living through a combat operation is no guarantee that a participant derived any significant insights." These experiences become useful to the doctrinal process only after they are recorded and available for review (5).

Combat Experience of Others. Holley points out several difficulties with the recorded combat experiences of foreign militaries. For example, one may encounter problems in gaining access to enough information to make useful generalizations. Consequently, Holley warns against deriving false inferences from limited or incomplete information. Further, if the information has to be translated into English, one must consider the factors of cost, time, and accuracy (5-6).

Full-Scale Maneuvers. The recorded results of maneuvers—defined by Holley as "two-sided, free-play practice with a panoply of all arms" (6)—are more applicable to the development of tactical than of operational doctrine. Information about maneuvers at the operational level of war would be more helpful to this study, but such data rarely addresses air base security operations.

Unit Exercises/Service Tests. Because unit exercises and service tests are generally conducted on a smaller scale than are maneuvers, they are less realistic than their full-scale counterparts. Holley believes that these exercises/tests can in fact produce useful information if the unit's commander is given adequate flexibility in conducting the exercise (7). However, like full-scale maneuvers, this source yields more information about tactics than operations and, therefore, is of limited usefulness in forming generalizations about air base security missions.

War Games/Command-Post Exercises. Holley again points out the importance of free play and initiative if war games and command-post exercises are to yield useful insights (7). In particular, war games tailored to a flexible, in-depth examination of air base security missions could provide useful information for the development of operational doctrine.

Systematic Bibliographic Searches. Holley emphasizes that agencies developing doctrine need to establish procedures for conducting a "continuous, comprehensive, and systematic bibliographic search of the available professional, historical, and technical literature." This source of information is essential if the doctrine is to remain current and applicable to real-world threats and conflicts (7-8). The numerous on-line com-

puterized data bases and service-school libraries are excellent bibliographic tools.

Liaison with Other Agencies. Holley also recommends "effective liaison" with a variety of military and civilian agencies, research activities, service schools, and civilian universities (8). This connection allows the agency that is writing doctrine to gain knowledge about doctrinal developments and instruction in other military branches and provides important information from civilian counterparts, such as federal, state, and local law enforcement agencies.

Phase 2: Formulation

The formulation phase objectively analyzes the collected information and makes generalizations about optimal approaches to operational procedures. Holley suggests that by adhering to scientific standards of logical development during this phase, one may avoid "hierarchical pressures" (8).

Analyze. Holley recommends a dialectic analysis that conducts "a systematic comparison of like experiences to identify the common patterns of success" while purposely looking for contradictory information that begs the question "why?" (9). Developers of doctrine must then reach a satisfactory resolution—a synthesis derived from the thesis of successful patterns and the antithesis of opposing information.

Draft Tentative Doctrinal Statement. After using the dialectic process to formulate sound generalizations, one must draft "tentative doctrinal statements." Holley believes that "the mere act of writing induces a certain precision" by revealing difficulties with doctrinal definitions that were inadequately formulated (9).

Verify with Trial Balloon. Once a tentative draft of the doctrine is ready, Holley advocates informally and unofficially soliciting reactions to the document through journal publication, peer review, and symposiums. Journal publication is useful because (1) it is unofficial and thus unattributable, (2) it evokes comments from unanticipated sources, and (3) it may initiate further productive dialogue that could lead to improvements and refinement of the doctrine (9). Further, circulating the draft doctrine among the developer's military contemporaries emulates the scientific community's peer-review process and can generate many valuable ideas, suggestions, and criticisms (10). Last, a military symposium consisting of audience-participation forums and formal panel discussions can also provide creative criticisms for improvement of the doctrine (10).

Reformulate Doctrinal Statement. After using the above methods to obtain informal feedback on the draft doctrine, one should refine the document by incorporating the suggestions that are most germane (10).

Phase 3: Dissemination

Holley stresses the importance of using factual support for the refined generalizations presented in the formal doctrine. Specifically, he charges

that "our doctrinal manuals may be fundamentally deficient in that they normally offer unadorned generalizations, pure doctrine, without supporting evidence, historical examples and the like to illustrate the experience on which the generalizations are based." If such supporting efforts are impractical, he urges that—at a minimum—the doctrine should include full documentation to allow others to follow the process of collection and formulation that led to its creation (11).

Applying Holley's Methodology to the Air Base Security Model

Holley's methodology provides a framework for establishing an effective process for doctrinal development. However, one needs a tool to ensure that the process examines the full range of operational activities required to achieve air base security. The multidimensional model of air base security developed previously in this study is such a tool. This model yields 64 potential categories created by the three-dimensional fusion of the various levels of threat and the portions of the spectrum of conflict with traditional operational missions. That is, 16 environmental categories are possible for each of the four air base security missions (law enforcement, system security, air base ground defense, and information security):

1. Basic threats, primary conflicts
2. Level I threats, primary conflicts
3. Level II threats, primary conflicts
4. Level III threats, primary conflicts
5. Basic threats, low-intensity conflicts
6. Level I threats, low-intensity conflicts
7. Level II threats, low-intensity conflicts
8. Level III threats, low-intensity conflicts
9. Basic threats, midintensity conflicts
10. Level I threats, midintensity conflicts
11. Level II threats, midintensity conflicts
12. Level III threats, midintensity conflicts
13. Basic threats, high-intensity conflicts
14. Level I threats, high-intensity conflicts
15. Level II threats, high-intensity conflicts
16. Level III threats, high-intensity conflicts

Identifying Sources for the Collection Phase

One should begin the process of doctrinal development by examining the sources recommended by Holley and identifying examples that fit each of the 64 categories of our model. If no examples exist for a particular category, one should create maneuvers, exercises, war games, or other forms of simulations—with actual forces or computer-generated forces—to

establish a body of information for the formulation phase. The collection phase might best be conducted by a military historian, preferably one with a background in air base security, or a specialist in library science who is proficient in military research. A historian could be placed at the Air Force Office of Security Police in Washington, D.C., or a curator/archivist at the Security Police Museum at Lackland AFB, Texas, and could begin the collection phase by examining the following material.

US Combat Experience. Two excellent historical sources are Roger P. Fox's *Air Base Defense in the Republic of Vietnam, 1961-1973* and Marie Shadden's unpublished "Security Police History: 1947-1982."⁵ Fox's book provides an overview of air base security efforts from World War I through the Vietnam conflict, with primary emphasis on the historical development of air base ground defense. His detailed discussion of the Vietnam conflict includes information that generally embraces all three levels of threat, low-to midintensity conflicts, and air base ground defense. Shadden's study provides information for most of our model's permutations with the exception of categories including high-intensity conflict. Both works cite additional bibliographic sources such as after-action reports of combat operations, weekly intelligence summaries, end-of-tour reports, documents from Project CHECO (contemporary historical examination of current operations) and Project Corona Harvest, DOD intelligence information reports, military annual histories, and a large variety of security police historical documents maintained in the archives at the Security Police Museum.⁶

Combat Experience of Others. The British Royal Air Force (RAF) Regiment conducts missions similar to those of US Air Force systems security and air base ground defense, so historical documentation of its activities may be helpful. Group Capt Kinsley M. Oliver's *A Short History of the RAF Regiment* is a good starting point.⁷

Full-Scale Maneuvers. Full-scale Air Force maneuvers generally include air base ground defense activities and focus on the mid- to high-intensity portion of the spectrum of conflict. Therefore, after-action and formal evaluation reports from these exercises may provide some useful grist for our doctrinal mill. Examples of full-scale maneuvers include (1) REFORGER, the joint/combined exercise that includes mobilization of CONUS forces to West Germany; (2) Team Spirit, a joint/combined military exercise conducted in South Korea; and (3) Brim Frost, another joint/combined military exercise conducted in Alaska.

Unit Exercises and Competitions. A variety of exercises and competitions involving air base security embodies a wealth of information for the collection phase. Although most of these events deal with tactics, one may nevertheless derive generalizations about the operational aspects of air base security. Similarly, even though the exercises usually focus on the air base ground defense mission, even minor aspects of system security, law enforcement, and information security can be illuminating to writers of doctrine. One event, the annual Security Police outstanding unit awards competition,

does in fact examine a full range of air base security activities, which are documented in the unit nomination submissions.

Examples of exercises include (1) Salty Demo, a full-blown air base survivability exercise conducted in the European theater of operations; (2) Desert Warrior, involving Security Police and other air base functional areas as well as US Army Special Forces operating in a semiarid bare-base environment in central Washington State; (3) Creek Warrior, a joint air base ground defense exercise conducted in Europe as part of the larger Allied Air Forces Cold Fire exercise; (4) Silver Flag Alpha, air base ground defense exercises conducted by the Tactical Air Command (TAC) in a desert environment at Nellis AFB, Nevada; and (5) Volant Scorpion, air base ground defense exercises conducted by the Military Airlift Command (MAC) in a woodland environment at Little Rock AFB, Arkansas.

Examples of competitions include (1) Peacekeeper Challenge, an annual worldwide Security Police competition that generally includes events in physical fitness, combat rifle, combat tactics, handgun, machine gun, grenade launcher, accident investigation, crime-scene investigation, military working dog, and information security; (2) Giant Sword, a Strategic Air Command bomber competition that incorporates system security events; and (3) Olympic Shield/Arena, a SAC missile combat competition that also incorporates system security events.

War Games/Command-Post Exercises. Computer- and board-oriented war games as well as various command-post exercises provide abstract information that may be applicable to air base security operational doctrine. Again, these activities often emphasize the air base ground defense mission due to the intrinsic nature of war games. However, that fact does not preclude the development of new games or simulations that address system security, law enforcement, or even information security. In the past, most software for computer war games was supported only by large mainframe or expensive minicomputer systems. Recently, though, an increasing amount of war-gaming software is designed to run on small computers such as the Zenith Z-248 systems obtained by the Air Force on the standard small computer contract, and many board-oriented war games have been converted to software versions. Additionally, the development of facilities such as the Air Force Wargaming Center will further expand the store of data available to developers of air base security doctrine.

Systematic Bibliographic Searches. Numerous bibliographical tools contain relevant information, especially in the area of law enforcement. For instance, the National Criminal Justice Reference Service (NCJRS) is readily accessible through several computer networks (e.g., Compuserve or Dialog).⁸ It lists US and international research reports, books, journals, newspaper and magazine articles, and audiovisual productions relating to a wide variety of law enforcement and criminal justice matters. The *Criminal Justice Periodical Index* provides similar information. Further, the Air University Library at Maxwell AFB, Alabama, has an on-line bibliographic system accessible by means of a standard computer terminal with

a 1200-baud modem, as do larger, civilian university libraries, usually at no cost to the user.⁹

Liaison with Other Agencies. The broad nature of operations in the four mission areas requires that doctrine writers maintain "effective liaison" with a number of agencies, including the Air Force Office of Special Investigations, the US Army Military Police, the International Association of Chiefs of Police, the American Society for Industrial Security, the Federal Bureau of Investigation (FBI), and the British RAF Regiment.

Suggested Steps for the Formulation Phase

Considering the large amount of data (40 years' worth) available for review, the objective analysis of the collected information on air base security will be a major undertaking. At least four people—one for each mission area—should conduct the formulation phase in conjunction with the historian/bibliographer(s) who completed the collection phase. They should analyze the collected data, using the threat/conflict/mission model to focus their efforts and Holley's dialectic approach to ensure sound formulation. Ultimately, they should produce well-supported generalizations about the optimum operational procedures for their mission area in each of the 16 categories of threat/conflict.

The logical location for the formulation team would be Headquarters AFOSP because of the availability of experts in each of the four traditional mission areas. An alternative approach would be to select four major commands (MAJCOMs), each having considerable experience in a particular mission (e.g., SAC for systems security, TAC for ABGD, Air Force Systems Command or Air Force Logistics Command for information security, and Air Training Command for law enforcement). Geographical separation of the team would probably not be detrimental to initial formulation activities, but dissemination of historical data by the archivist to team members would be more difficult in such a decentralized arrangement. Because of the potential for overlap (e.g., C³ in law enforcement, security, and ABGD), members should exchange drafts or hold periodic meetings to avoid duplication and maintain a consistent terminology. When the members complete their tentative doctrinal statements, they should meet to conflate them into a single document.

The complete draft should be sent to Security Police units and MAJCOMs for informal review and comment. Although the length of the document would probably preclude full publication in any journal, the main doctrinal concepts could be incorporated in an article for *Security Police Digest* or *Airpower Journal*. These concepts could also be presented in a symposium format at AFOSP or one of the Worldwide Security Police symposiums. Further, a symposium at the Air University Center for Aerospace Doctrine, Research, and Education—or, more specifically, the Airpower Research Institute—would stimulate ideas and comments from the operational world and other combat support functions. The doctrine development team

should then revise their draft in accordance with the most useful of these suggestions/criticisms, thus completing the informal stage of the formulation process.

The Official Dissemination Phase

The formal aspects of the formulation phase and the particulars of the dissemination phase are spelled out in the new AFR 1-2, which should be published by the time this study appears.¹⁰ One of the first requirements of the regulation is that the office of primary responsibility (OPR) develop a draft outline of the doctrine.¹¹ Without a full-scale collection effort, this requirement may be difficult to satisfy; nevertheless, one may speculate about the types of things to include in this outline (see appendix B).

Conclusion

The goal of my research has been to recommend a practical methodology for developing an operational doctrine for air base security. Toward that end, this study postulates a doctrinal model based on four levels of threat, four segments of the spectrum of conflict, and four traditional missions that pertain to air base security. This model focuses the collection of data needed to develop a comprehensive doctrine by creating 64 boxes into which information on air base security operations can be placed. Some of the categories will have a great deal of information, many will have information in common with other categories, and others will have little or no information. For those categories for which there is no precedent, we will have to create theoretical constructs and test them. More than likely, this process will be a lengthy one to ensure an adequate description of air base security operations. Nevertheless, the Air Force now has a systematic methodology for writing a doctrine of air base security that it has long needed.

Notes

1. Maj Gen I. B. Holley, Jr., "The Doctrinal Process: Some Suggested Steps," *Military Review* 59, no. 4 (April 1979): 4-5.

2. Maj Gen I. B. Holley, Jr., USAFR, Retired, "Concepts, Doctrines, Principles: Are You Sure You Understand These Terms?" *Air University Review* 35, no. 5 (July-August 1984): 91.

3. *Ibid.*, 92.

4. *Ibid.*, 91.

5. Roger P. Fox, *Air Base Defense in the Republic of Vietnam, 1961-1973* (Washington, D.C.: Government Printing Office, 1979); Capt Marie Shadden, "Security Police History: 1947-1982" (Lackland AFB, Tex.: US Air Force Security Police Academy, 1984).

6. Both Fox and Shadden used these sources extensively.

7. Group Capt Kinsley M. Oliver, *A Short History of the RAF Regiment* (London: Her Majesty's Stationery Office, 1968).

8. I have been able to access data from the NCJRS through Compuserve's IQuest service with my home computer and through Dialog at the Michigan State University library.

9. I did many of my bibliographic searches for this study with my home computer, using the Air University Library's system.

10. AFR 1-2, "Assignment of Responsibilities for Development of Aerospace Doctrine," June 1988 (draft), 31-35.

11. *Ibid.*, 31.

APPENDIXES

APPENDIX A

Definitions of Doctrine

Excerpts from official manuals and doctrinal literature indicate the difficulty of writing a concise, authoritative definition for the term *doctrine*.

Official Definitions

Operational doctrine: "The proper use of aerospace forces in the context of distinct objectives, force capabilities, broad mission areas, and operational environments. . . . Describes the organization of aerospace forces, and it anticipates changes and influences which may affect military operations, such as technological advances. . . . Provide[s] detailed mission descriptions and methods for preparing and employing aerospace forces." AFM 1-1, *Basic Aerospace Doctrine of the United States Air Force*, 16 March 1984, vi.

- "(1) Describes aerospace missions and tasks within operating environments.
- (2) Guides combat commanders.
- (3) Guides weapons development programs and force planning.
- (4) Provides foundation for Air Force contributions to joint and combined doctrine development." AFR 1-2, "Assignment of Responsibilities for the Development of Aerospace Doctrine," June 1988 (draft), 2.

Definitions from Literature

"Military doctrine . . . is what is officially understood to be the best way to do military things. It can be at once authoritative and opinionative. To be effective as a guiding force, it has to be both widely taught and widely believed. It can deal with such divergent challenges as how to best employ a particular weapon system, and how to organize a particular group of warriors for optimum usefulness." Col John P. Brancaio, "In Search of Command and Staff Doctrine," *Air Force Law Review*, 1988, 2.

"Military doctrine does constitute the conceptual skeleton upon which are mounted the sinews of materiel, the muscles of battalions and brigades and the nervous system of planning and policy decision. . . . It is useful to

understand doctrine as being the officially sanctioned theory of victory outlining the conduct of war on all levels, from the broadest aspects of operational planning down through tactics and standard operating procedures to the most minor details of squad patrolling. Generally, doctrine is historically derived, in that it is the synthetic product of actual experience in previous conflicts. While doctrine can be altered with the advent of new weapons or new technologies of communication and transportation or according to the demands arising from a new conflict, the doctrine in effect prior to the start of a war powerfully conditions the military and civilian perceptions and decisions which lead to the onset of hostilities." Larry E. Cable, *Conflict of Myths: The Development of American Counterinsurgency Doctrine and the Vietnam War* (New York: New York University Press, 1986).

"Informal doctrine is the result of repeated experiences that produce similar results and subsequently produce beliefs—sometimes personal, sometimes broadly held—about what usually works best. . . . These informal beliefs are more timely, more accurate, and more useful than officially sanctioned doctrine, which must suffer through the travails of bureaucratic coordination and compromise before publication. On the other hand, informal doctrinal beliefs may not be accurate and useful. Those who hold such beliefs may have an experience base that is shallow [and it] might also be too narrow. The doctrine development process must evaluate informal doctrine and separate the wheat from the chaff. Well-founded informal doctrinal beliefs must be sorted out. . . . The official doctrine that results from the development process becomes the vehicle for inculcating well-founded beliefs throughout the force. Thus, those who develop and publish official doctrine face a difficult task and bear a critically important responsibility. Although it is difficult to translate field experience and the doctrinal beliefs derived therefrom directly into the more abstract levels of doctrine, operational doctrine should issue directly from generalizations based on field experience." Col Dennis M. Drew, "Informal Doctrine and the Doctrinal Process: A Response," *Air University Review* 35, no. 6 (September–October 1984): 96–97.

"If doctrine's first function is to provide a tempered analysis of experience and thus a determination of what we believe, the second function must be to teach these beliefs or lessons to successors. . . . Organizational doctrine will discuss roles and missions assigned to an organization, current objectives, administrative organization, force-employment principles as influenced by the current situation, and, in some instances, tactics. . . . Organizational doctrine is very narrow in scope. . . . Organizational doctrine concerns the use of particular forces in a particular environment at a particular time—today. Organizational doctrine is current and thus tends to change relatively frequently in order to remain 'current.' Doctrine should provide guidance for actions, particularly important in the heat of combat

when direction from superiors may be unavailable. Three fundamental doctrinal functions: provide analysis of experience, teach beliefs/lessons to successors, and provide guidance for actions." Lt Col Dennis M. Drew, "Of Trees and Leaves: A New View of Doctrine," *Air University Review* 33, no. 2 (January-February 1982): 42-46.

"A fundamental problem with AF doctrine is the absence of any real consensus as to what doctrine is and just what it is supposed to do. The inability of AF people to understand the essence and purpose of doctrine is largely the result of trying to include too much under one umbrella word. Air Force doctrine is the body of enduring principles, the general truths and accepted assumptions, which provide guidance and a sense of direction on the most effective way to develop, deploy, and employ air power. It should not encompass either political influences or specific instructions on the execution of these principles. Doctrine offers a conceptual framework and way of thinking that provides general guidance to use in special situations. It provides the foundation, the starting point, on which every aspect of the AF should be based, including force structure, strategy and tactics, training, and functional procedures. . . . Doctrine acts as a sounding board, as a frame of reference for testing, evaluating, and employing not only new concepts but also new technological developments and new policies. . . . Doctrine provides the rationale behind both the organization and employment of air forces. Doctrine is a compass, not a road map. It gives us the general heading, but it does not give us detailed instructions on how to get there. It provides direction but not the details of how to meet the demands of a particular situation. . . . We must avoid the temptation to focus our attention too closely on the type of war we anticipate and are most capable of fighting and to ignore those types in which we do not expect to become involved. Our doctrine and the procedures for implementing it must prepare us for a full spectrum of conflict. To be of value, doctrine must meet three criteria: it must be understood; it must be valid; and it must be translated into action. One important way to assure that the principles which comprise our doctrine are correct is to base them on an objective analysis of a broad range of historical experience." Maj Robert C. Ehrhart, "Some Thoughts on Air Force Doctrine," *Air University Review* 31, no. 3 (March-April 1980): 30-38.

"If we expect success in battle, every AF officer must understand our basic views about war to the extent that even the most junior among us can conduct meaningful operations instinctively in the absence of C³. Real war demands no less. . . . AFM 1-1 ignores the Clausewitzian admonition that the profound act of judgment is to establish, at the outset, the type of war upon which one is embarking. . . . There is only one real issue, and that is war; and the sole purpose of doctrine is to convey our collective and institutional response to it. . . . Procedures are important . . . but they are

not doctrine. [In] a real war . . . nothing will go according to plan. [Thus,] intuitive judgment and mental flexibility will be absolutely essential, and improvisation and risk-taking will be the only way to contend with the constantly changing conditions of battle. Under these circumstances, what would be the utility of the knowledge found in a procedures manual disguised as doctrine? If one understands war, he implicitly understands doctrine; without understanding war, doctrine becomes an army of abstract words and phrases searching for a unifying idea. . . . If our tasks in the U.S. Air Force are to prepare for war, deter it if possible, and fight it successfully across a spectrum of conflict, then we must understand war, make war the basis of our doctrine, and teach war to our officers." Col Thomas A. Fabyanic, USAF, Retired, "War, Doctrine, and the Air War College," *Air University Review* 37, no. 2 (January-February 1986): 16-26.

"Doctrine can be an overriding determinant of combat outcomes. . . . Doctrine-as-implicit-orientation highlights the tacit nature of the assumptions and beliefs by which combatants fail or succeed. . . . The precepts that count most in the heat of battle are those that have become more or less second nature. This reality obviously places a heavy burden on everyone in military uniform to master the craft of warfighting. . . . The doctrine that really wins or loses wars is the collection of internalized values, rules of thumb, and elemental images of war on which a military group instinctively relies in battle. . . . Doctrine then boils down to what is known to work where it counts—in combat. . . . We must never forget that the ultimate arbiter of doctrinal beliefs is whether they help us to prevail." Lt Col Barry D. Watts and Maj James O. Hale, "Doctrine: Mere Words, or a Key to War-Fighting Competence?" *Air University Review* 35, no. 6 (September-October 1984): 4-13.

"Doctrine is what is being taught, i.e., rules or procedures drawn by competent authority. Doctrines are precepts, guides to action, and suggested methods for solving problems or attaining desired results. Doctrine . . . is an officially approved teaching based on accumulated experience. . . . A doctrine is a generalization based on sufficient evidence to suggest that a given pattern of behavior will probably lead to the desired result. While a concept is tentative and speculative, a doctrine is more assured. Doctrines are akin to rules, precepts or maxims, or a set of operations or moves reduced to more or less uniform procedures for meeting specific types of problems. . . . Doctrine [is] that mode of approach which repeated experience has shown usually works best. . . . Doctrines are derived by generalization . . . principles are derived by abstraction. With doctrine, the thrust is on 'how to do it.'" Maj Gen I. B. Holley, Jr., USAFR, Retired, "Concepts, Doctrines, Principles: Are You Sure You Understand These Terms?" *Air University Review* 35, no. 5 (July-August 1984): 90-93.

"Since there is no best doctrine (only a better one), AF doctrine will never be complete or finished. Effective doctrine should be neither as solid as granite nor as shifting as the sands of the desert. Rather, it must be reflective of past lessons learned, yet open to refinement and growth." Col Clifford R. Krieger, "USAF Doctrine: An Enduring Challenge," *Air University Review* 35, no. 6 (September-October 1984): 22.

"One of the critical factors facing modern military organizations is the articulation of doctrine: the conceptual framework within which one plans and trains one's forces in peace and war so that they reach maximum effectiveness in battle. Doctrine is particularly important in giving commanders and subordinates on the battlefield a set of shared assumptions that enable them to know intuitively what others might be doing under the confused pressures of combat." Williamson Murray, "A Tale of Two Doctrines: The Luftwaffe's 'Conduct of the Air War' and the USAF's Manual 1-1," *The Journal of Strategic Studies* 6, no. 4 (December 1983): 84-91.

APPENDIX B

Air Base Security Operational Doctrine

(AFM 2-XZ): A Suggested Outline

I. Introduction

- A. Definition**
- B. Development Process**
- C. Scope of Manual**

II. Distinct Objectives

A. Apply Basic Doctrine Principles

- 1. Security**
- 2. Realistic Objectives**
- 3. Offensive: Act, Not React**
- 4. Surprise**
- 5. Balance Mass/Economy of Force**
- 6. Maneuver**
- 7. Timing and Tempo**
- 8. Unity of Command**
- 9. Simplicity**
- 10. Logistics**
- 11. Cohesion**

B. Ensure Air Base Operability

- 1. Protect and Defend Personnel**
- 2. Protect and Defend Resources**
- 3. Ensure Sortie Generation**

- III. Force Capabilities
 - A. To Meet Objectives/Principles
 - B. To Counter Threats
 - 1. Basic Threats
 - 2. Level I Threats
 - 3. Level II Threats
 - 4. Level III Threats
 - C. Development
 - 1. Resources
 - a. Economic
 - (1) Acquisition/Procurement
 - (2) Operations and Maintenance
 - b. Force Structure
 - (1) Officer
 - (2) Enlisted
 - (3) Civilian
 - c. Training
 - (1) Doctrinal Principles
 - (2) Objectives
 - (3) Missions
 - d. Equipment
 - (1) Mission Oriented
 - (2) Functional
 - (3) Reliability
 - e. Information
 - (1) Force Management
 - (2) Intelligence
 - (3) Analysis
 - (4) Administration

- 2. Technology
 - a. Enhance Capabilities
 - b. Force Multiplying
 - c. Balanced against Threat
- D. Deployment
 - 1. Reduced Response Time
 - 2. Increased Readiness
 - 3. Vulnerability of Position
 - 4. Flexible Force Utilization
- E. Force Employment
 - 1. Location
 - 2. Defensive
 - 3. Offensive
 - 4. Threat Oriented
- F. Force Coordination
 - 1. Operational Planning
 - 2. Risk Management
 - 3. Counter-Threat Prioritization
- IV. Operational Environments: Conflict Spectrum and Threat Levels
 - A. Primary Conflicts
 - 1. Patrol/Fire Team Responses (Basic, Level I Threats)
 - 2. Arrests/Apprehensions (Basic, Level I Threats)
 - 3. Hostage Situations (Basic, Level I Threats)
 - 4. Protest/Riot Control (Basic, Level I Threats)
 - 5. Traffic Accident Response (Basic, Level I Threats)
 - 6. Espionage Incident (Basic, Level I Threats)
 - B. Low-Intensity Conflicts (High Probability Conflicts)
 - 1. Insurgency/Counterinsurgency (Basic, Level I and II Threats)
 - 2. Combatting Terrorism (Basic, Level I Threat)

3. Peacekeeping Operations (Basic, Level I, II, III Threats)
4. Peacetime Contingency Operations (Basic, Level I, II, III Threats)

C. Midintensity Conflicts

1. Limited Conventional War (Basic, Level I, II, III Threats)
2. General Conventional War (Basic, Level I, II, III Threats)

D. High-Intensity Conflicts

1. Nuclear War (Basic, Level I, II, III Threats)
2. Postnuclear Environment (Basic, Level I, II, III Threats)

V. Broad Mission Areas

A. Historically Based Missions

1. Law Enforcement

a. Administration and Reports

- (1) Reports and Analysis
- (2) Pass and Registration
- (3) Information Security Administration

b. Operations

- (1) Command, Control, and Communications
- (2) Resource Protection
- (3) Installation Patrol
- (4) Installation Entry
- (5) Detention
- (6) Investigation
- (7) Emergency Services Teams
- (8) Protest/Riot Control

2. Information Security

- a. Security Education/Motivation
- b. Classification Management
- c. Personnel Security
- d. Industrial Security

- e. Wartime Information Security Programs
- f. Computer Security
- g. Communications Security
- h. Operations Security
- 3. Systems Security
 - a. Fire Team Force Structure
 - b. Command, Control, and Communications
 - (1) Redundancy
 - (2) Reporting and Alerting
 - c. Security Priorities
 - d. Security Facilities/Areas
 - e. Intrusion Detection
 - f. Circulation Control
 - g. Response Options
 - h. Operations
 - (1) Aircraft
 - (2) Missile
 - (3) Nuclear Weapon
 - (4) Command, Control and/or Warning
- 4. Air Base Ground Defense
 - a. Fire Team Force Structure
 - b. Command, Control, Communications, and Intelligence/Counterintelligence
 - (1) Interoperability with Army and Host-Nation Forces
 - (2) Redundancy
 - (3) Clearly Established Transition Points
 - c. Internal Defense: Close Defense Area
 - (1) Patrols
 - (2) Tactical Sensors

(3) Denial Systems: Mines, Obstacles, Etc.

(4) Observation/Listening Posts

(5) Defensive Positions

(6) Host-Nation Interface

(7) Rally Points/Assembly Areas

d. External Defense: Main Defense Area

(1) Timing

(a) Alert Stages

(b) Intelligence Indicators

(2) Joint Service Agreement (Army)

(3) OPCON Air Base Command and Control/CSP
(Level I and II Threats)

(4) Host-Nation Support

B. Theoretically Based Missions

1. Derived from Strategic Planning

2. Contingency Operations

3. Joint Operations

4. Combined Operations

Glossary

ABGD	air base ground defense
AFM	Air Force manual
AFOSP	Air Force Office of Security Police
AFP	Air Force pamphlet
AFR	Air Force regulation
Baud	Speed at which a computer transmits serial data; 1200 baud is roughly equivalent to 120 characters per second.
BDOC	base defense operations center
C ³	command, control, and communications
C ³ I	command, control, communications, and intelligence
CAS	close air support
CHECO	contemporary historical examination of current operations
COMPUSEC	computer security
COMSEC	communications security
CONUS	continental United States
DOD	Department of Defense
FBI	Federal Bureau of Investigation
FEBA	forward edge of the battle area
FM	field manual
ICBM	intercontinental ballistic missile
IDAD	internal defense and development
IDS	intrusion detection system
JCS	Joint Chiefs of Staff
JSA	Joint Service Agreement
LIC	low-intensity conflict

MAC	Military Airlift Command
MAJCOM	major command
NBC	nuclear, biological, chemical
NCJRS	National Criminal Justice Reference Service
NCO	noncommissioned officer
OPR	office of primary responsibility
OPSEC	operations security
OSI	Office of Special Investigations
RAF	Royal Air Force
REFORGER	Return of Forces to Germany
SAC	Strategic Air Command
SAM	surface-to-air missile
SORTS	status of resources and training system
TAC	Tactical Air Command
UCMJ	Uniform Code of Military Justice